WE CLAIM:

1. A computer program product for controlling a computer to detect malware, said computer program product comprising:

detecting logic operable to detect a file access request to a computer file by a requesting computer;

file access clearance request generating logic operable to generate a file access clearance request including data identifying said computer file;

file access clearance request transmitting logic operable to transmit said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware;

file access clearance response receiving logic operable to receive at said requesting computer a file access clearance response from said assessment computer; and

file access permitting logic operable if said file access clearance response indicates said computer file does not contain malware, to permit said file access request by said requesting computer.

2. A computer program product as claimed in claim 1, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

3. A computer program product as claimed in claim 1, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

4. A computer program product as claimed in claim 1, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then computer file transmitting logic is operable to transmit said computer file from said requesting computer to said assessment computer.

5. A computer program product as claimed in claim 1, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer.

6. A computer program product as claimed in claim 1, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

7. A computer program product for controlling a computer to detect malware, said computer program product comprising:

file access request receiving logic operable to receive at an assessment computer a file access clearance request from a requesting computer, said file access clearance request including data identifying a computer file to be accessed by said requesting computer;

file access clearance response generating logic operable in dependence upon said data identifying said computer file to determine if said computer file has previously been assessed as not containing malware and to generate a file access clearance response; and

file access clearance response transmitting logic operable to transmit said file access clearance response to said requesting computer.

8. A computer program product as claimed in claim 7, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

9. A computer program product as claimed in claim 7, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

10. A computer program product as claimed in claim 7, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then computer file receiving logic is operable to receive at said assessment

computer said computer file from said requesting computer and performing a malware scan of said computer file.

11. A computer program product as claimed in claim 7, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer.

12. A computer program product as claimed in claim 7, wherein said assessment computer stores a database of computer files previously assessed as to whether they contain malware.

13. A computer program product as claimed in claim 12, wherein said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations.

14. A computer program product as claimed in claim 7, wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to greater range of computer files when operating in said higher level security mode compared with said lower level security mode.

15. A computer program product as claimed in claim 14, wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer.

16. A computer program product as claimed in claim 7, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

17. A computer program product for controlling a computer to detect malware, said computer program product comprising:

file access request detecting logic operable to detect a file access request to a computer file by a requesting computer;

file access clearance request generating logic operable to generate a file access clearance request including data identifying said computer file;

file access clearance request transmitting logic operable to transmit said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware;

file access clearance request receiving logic operable to receive at said assessment computer said file access clearance request from a requesting computer;

file access clearance response generating logic operable in dependence upon said data identifying said computer file to determine if said computer file has previously been assessed as not containing malware and to generate a file access clearance response;

file access clearance response transmitting logic operable to transmit said file access clearance response to said requesting computer;

file access clearance response receiving logic operable to receive at said requesting computer said file access clearance response from said assessment computer; and

file access permitting logic operable if said file access clearance response indicates said computer file does not contain malware to permit said file access request by said requesting computer.

18. A computer program product as claimed in claim 17, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

19. A computer program product as claimed in claim 17, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

20. A computer program product as claimed in claim 17, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then computer file transmitting logic is operable to transmit said computer file from said requesting computer to said assessment computer, receiving at said assessment computer said computer file from said requesting computer and performing a malware scan of said computer file.

21. A computer program product as claimed in claim 17, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer.

22. A computer program product as claimed in claim 17, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer.

23. A computer program product as claimed in claim 17, wherein said assessment computer stores a database of computer files previously assessed as to whether they contain malware.

24. A computer program product as claimed in claim 23, wherein said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations.

25. A computer program product as claimed in claim 17, wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to greater range of computer files when operating in said higher level security mode compared with said lower level security mode.

26. A computer program product as claimed in claim 25, wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer.

28. A computer program product as claimed in claim 17, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

29. A method of detecting malware, said method comprising the steps of:

detecting a file access request to a computer file by a requesting computer;

generating a file access clearance request including data identifying said computer file;

transmitting said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware;

receiving at said requesting computer a file access clearance response from said assessment computer; and

if said file access clearance response indicates said computer file does not contain malware, then permitting said file access request by said requesting computer.

30. A method as claimed in claim 29, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

31. A method as claimed in claim 29, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

32. A method as claimed in claim 29, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then transmitting said computer file from said requesting computer to said assessment computer.

33. A method as claimed in claim 29, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer.

34. A method as claimed in claim 29, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

35. A method of detecting malware, said method comprising the steps of:

receiving at an assessment computer a file access clearance request from a requesting computer, said file access clearance request including data identifying a computer file to be accessed by said requesting computer;

in dependence upon said data identifying said computer file determining if said computer file has previously been assessed as not containing malware and generating a file access clearance response; and

transmitting said file access clearance response to said requesting computer.

36. A method as claimed in claim 35, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

37. A method as claimed in claim 35, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

38. A method as claimed in claim 35, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then receiving at said assessment computer said computer file from said requesting computer and performing a malware scan of said computer file.

39. A method as claimed in claim 35, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer.

40. A method as claimed in claim 35, wherein said assessment computer stores a database of computer files previously assessed as to whether they contain malware.

41. A method as claimed in claim 40, wherein said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations.

42. A method as claimed in claim 35, wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to greater range of computer files when operating in said higher level security mode compared with said lower level security mode.

43. A method as claimed in claim 35, wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer.

44. A method as claimed in claim 35, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

45. A method of detecting malware, said method comprising the steps of:

detecting a file access request to a computer file by a requesting computer;

generating a file access clearance request including data identifying said computer file;

transmitting said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware;

receiving at said assessment computer said file access clearance request from a requesting computer;

in dependence upon said data identifying said computer file determining if said computer file has previously been assessed as not containing malware and generating a file access clearance response;

transmitting said file access clearance response to said requesting computer;

receiving at said requesting computer said file access clearance response from said assessment computer; and

if said file access clearance response indicates said computer file does not contain malware, then permitting said file access request by said requesting computer.

46. A method as claimed in claim 45, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

47. A method as claimed in claim 45, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

48. A method as claimed in claim 45, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then transmitting said computer file from said requesting computer to said assessment

computer, receiving at said assessment computer said computer file from said requesting computer and performing a malware scan of said computer file.

49. A method as claimed in claim 45, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer.

50. A method as claimed in claim 45, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer.

51. A method as claimed in claim 45, wherein said assessment computer stores a database of computer files previously assessed as to whether they contain malware.

52. A method as claimed in claim 51, wherein said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations.

53. A method as claimed in claim 45, wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to greater range of computer files when operating in said higher level security mode compared with said lower level security mode.

54. A method as claimed in claim 53, wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer.

55. A method as claimed in claim 45, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

56. Apparatus for detecting malware, said apparatus comprising:

a detector operable to detect a file access request to a computer file by a requesting computer;

a file access clearance request generator operable to generate a file access clearance request including data identifying said computer file;

a file access clearance request transmitter operable to transmit said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware;

a file access clearance response receiver operable to receive at said requesting computer a file access clearance response from said assessment computer; and

a file access permission unit operable if said file access clearance response indicates said computer file does not contain malware, to permit said file access request by said requesting computer.

57. Apparatus as claimed in claim 56, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

58. Apparatus as claimed in claim 56, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

59. Apparatus as claimed in claim 56, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then a computer file transmitter is operable to transmit said computer file from said requesting computer to said assessment computer.

60. Apparatus as claimed in claim 56, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer.

61. Apparatus as claimed in claim 56, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

62. Apparatus for controlling a computer to detect malware, said apparatus comprising:

a file access request receiver operable to receive at an assessment computer a file access clearance request from a requesting computer, said file access clearance request including data identifying a computer file to be accessed by said requesting computer;

a file access clearance response generator operable in dependence upon said data identifying said computer file to determine if said computer file has previously been assessed as not containing malware and to generate a file access clearance response; and

a file access clearance response transmitter operable to transmit said file access clearance response to said requesting computer.

63. Apparatus as claimed in claim 62, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

64. Apparatus as claimed in claim 62, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

65. Apparatus as claimed in claim 62, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then a computer file receiver is operable to receive at said assessment

computer said computer file from said requesting computer and performing a malware scan of said computer file.

66. Apparatus as claimed in claim 62, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer.

67. Apparatus as claimed in claim 62, wherein said assessment computer stores a database of computer files previously assessed as to whether they contain malware.

68. Apparatus as claimed in claim 67, wherein said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations.

69. Apparatus as claimed in claim 62, wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to greater range of computer files when operating in said higher level security mode compared with said lower level security mode.

70. Apparatus as claimed in claim 69, wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer.

71. Apparatus as claimed in claim 62, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied.

72. Apparatus for controlling a computer to detect malware, said apparatus comprising:

a file access request detector operable to detect a file access request to a computer file by a requesting computer;

a file access clearance request generator operable to generate a file access clearance request including data identifying said computer file;

a file access clearance request transmitter operable to transmit said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware;

a file access clearance request receiver operable to receive at said assessment computer said file access clearance request from a requesting computer;

a file access clearance response generator operable in dependence upon said data identifying said computer file to determine if said computer file has previously been assessed as not containing malware and to generate a file access clearance response;

a file access clearance response transmitter operable to transmit said file access clearance response to said requesting computer;

a file access clearance response receiver operable to receive at said requesting computer said file access clearance response from said assessment computer; and

a file access permission unit operable if said file access clearance response indicates said computer file does not contain malware to permit said file access request by said requesting computer.

73. Apparatus as claimed in claim 72, wherein said data identifying said computer file includes a checksum value calculated from said computer file.

74. Apparatus as claimed in claim 72, wherein said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file.

75. Apparatus as claimed in claim 72, wherein if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then a computer file transmitter is operable to transmit said computer file from said requesting computer to said assessment computer, receiving at said assessment computer said computer file from said requesting computer and performing a malware scan of said computer file.

76. Apparatus as claimed in claim 72, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer.

77. Apparatus as claimed in claim 72, wherein if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer.

78. Apparatus as claimed in claim 72, wherein said assessment computer stores a database of computer files previously assessed as to whether they contain malware.

79. Apparatus as claimed in claim 78, wherein said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations.

80. Apparatus as claimed in claim 72, wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to greater range of computer files when operating in said higher level security mode compared with said lower level security mode.

81. Apparatus as claimed in claim 80, wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer.

5

82. Apparatus as claimed in claim 72, wherein a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied